

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Samuel K. Moore being duly sworn, depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Knoxville Division, Chattanooga, Tennessee Resident Agency. I have been employed as a Special Agent for 9 years. I have investigated federal criminal violations related to counter-terrorism, domestic terrorism, criminal enterprise, human trafficking, and crimes against children. I have received formal training and have participated in numerous search warrants in a variety of investigative matters. As a federal agent, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.
2. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement agencies and partners, and on my experience and training as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of interstate commerce, Title 18, United States Code, Sections 2252(a)(2) and 2252A(a)(2), which make it a crime to receive or distribute child pornography in interstate commerce and Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography.

3. This affidavit is being submitted in support of an application for a search warrant to search the following premises at 6303 Champion Road, Chattanooga, Tennessee 37416 (herein referred to as the Subject Premises) which is more fully described in Attachment B of this affidavit.
4. This affidavit will show there is probable cause that records and other items related to the violations being investigated (as specifically described in Attachment A, attached hereto and incorporated herein) will be found at the Subjects Premises.

APPLICABLE LAW

5. Title 18, United States Code, Sections 2252(a)(2) and 2252A(a)(2), make it a federal crime for any person to knowingly receive or distribute child pornography that has traveled in interstate or foreign commerce.
6. Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B), make it a federal crime for any person to knowingly possess any material that contains an image of child pornography that has been mailed, or shipped, or transported in interstate foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped, or transported in interstate or foreign commerce by any means, including by computer.
7. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. In addition to electronic communications, a computer user's Internet activities generally leave traces in the web cache and history files of the browser used. A forensic examiner can often recover

evidence which shows that a computer contains peer to peer software (P2P), when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. A person interested in sharing child pornography with others in the P2P network, need only place those files in his/her “shared” folder(s). Those child pornography files are then available to all users of the P2P network for download regardless of their physical location.

8. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user’s computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user’s computer without his/her active participation.

THE INVESTIGATION

9. On November 20th, 2018, SA Samuel Moore was reviewing a listing on ICACCOPS of the top child pornography P2P offenders in the Hamilton County, Tennessee area. ICACCOPS is a system put in place by various authorities to allow for the dissemination of data on P2P users who are sharing child pornography material on these networks.

The top offender in Hamilton County, Tennessee, pertaining to the ICACCOPS activity report revealed IP address 66.85.225.9 as a current downloader and possessor of a high amount of child pornography (2792 Files of Interest, 1848 Severe Files with 27 downloads from 8 separate investigators). ICACOPS detailed a large quantity of the material severity level 9 indicating material of pre-pubescent children, infant and pre-teen, being sexually assaulted. On November 20th, 2018, SA Moore contacted one of the investigators who had downloaded material from this IP address, Michael Foster an investigator with the Spring Hill, Tennessee Police Department, who stated that he had downloaded content on November 13th, 2018 at 10:51:20am from this IP address and verified the content of the material as child pornography.

10. On December 4th, 2018, SA Moore reached out to a second investigator, Lt. Scott Levasseur of the Dickson County, Tennessee Sheriff's Office who was found to have also downloaded child pornography from IP address 66.85.225.9, and Lt. Levasseur provided the following: On Monday, November 12, 2018, Lt. Levasseur was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device at IP address 66.85.225.9, because it was associated with a torrent with the infohash: *f97b5ac2e41687c8bd4cfa78f441fa63af82751*. This torrent file references 4669 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 66.85.225.9, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -BT7a4S- BitTorrent 7.10.4, and on Monday, November 12, 2018, between 0437 hrs and 0559 hrs, a download was

successfully completed of 1780 file(s) that the device at IP address 66.85.225.9 was making available. The device at IP Address 66.85.225.9 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

11. On December 5th, 2018, SA Moore reached out to a third investigator, Detective (Det.) Shane Lewis of the Gastonia, North Carolina Police Department, who had also downloaded material from this IP address and he provided the following: On Saturday, November 10, 2018, Det. Lewis was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Det. Lewis directed investigative focus to a device at IP address 66.85.225.9, because it was associated with a torrent with the infohash: 7f97b5ac2e41687c8bd4cfa78f441fa63af82751. This torrent file references 4669 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. Using a computer running investigative BitTorrent software, Det. Lewis directly connected to the device at IP address 66.85.225.9, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -BT7a4S- BitTorrent 7.10.4 and between 0211 hrs and 0240 hrs, Det. Lewis successfully completed the download of 918 file(s) that the device at IP address 66.85.225.9 was making available. The device at IP Address 66.85.225.9 was the sole candidate for each download, and as such, each files was downloaded directly from this IP Address.

12. Investigation determined EPB holds the registration on IP address 66.85.225.9. Subsequently, a United States Department of Justice administrative subpoena was submitted to EPB requesting subscriber information for the user of 66.85.225.9 during the timeframe of downloads obtained by the investigative personnel.

13. Results from the administrative subpoena indicated the subscriber was THOMAS PALIANI, 6303 Champion Road, Chattanooga, Tennessee 37416, telephone number 443-333-2755. The service is residential high speed internet that was initiated March 10th, 2017, in PALIANI's name. The email address for the account is shygyetn@yahoo.com.
14. Further investigation discovered that PALIANI is a registered sex offender, ID S0010113, and was a prior service U.S. Army soldier. PALIANI had joined the U.S. Army Feb 26, 2007, and in 2009 fell under investigation from CID for sexual exploitation. After an investigation and search of PALIANI's digital media it was revealed he possessed and viewed 58 videos of child pornography and over 1900 child pornography images. PALIANI was convicted and then subsequently incarcerated in the Joint Regional Correctional Facility SW San Diego from April 1, 2011-Feb 27, 2013, then received a Bad Conduct Discharge from the army.
15. Additional investigation revealed that in on-line forums, PALIANI has offered feedback and guidance on Webcams and video devices that can be attached to LG phones and computers, and upon driving by PALIANI's residence toys indicative of smaller children could physically be observed in the yard raising additional concerns of PALIANI's access to children and possible child pornography production concerns. Additionally, a Router/WiFi surveillance was conducted in areas in close proximity to PALIANI's residence which detailed a series of networks which were all secure and password protected, making it very unlikely someone other than PALIANI is utilizing that network and IP at time of downloads.

16. The following files and descriptions are images that were downloaded by IP address 66.85.225.9 are only a brief sampling of the material that was discovered, and many were found to have been downloaded on separate days and timeframes:

File Name	Description
000204.jpg	Male ejaculating on infant female
000215.jpg	Erect penis pressed against infants genitals
000221.jpg	Penis inserted into toddler age female
000227.jpeg	Penis inserted into toddler age female
000465.jpg	Bottle inserted into infant vagina
000492.jpg	Child bound and gagged with object inserted into vagina
000531.jpeg	Penis inserted into anal cavity of female infant

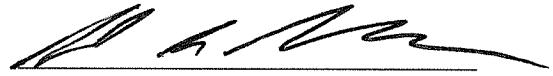
17. Tennessee Department of Motor Vehicles (DMV) indicated THOMAS S. PALIANI currently has a Tennessee driver's license number 096504357. The driver's license was issued on October 13th, 2014 and expires on December 26th, 2018. A 2004 red Pontiac Sunfire (GA) RDT0101 was found to be registered to PALIANI, which has been observed at 6303 Champion Road, Chattanooga, Tennessee, 37416 on multiple occasions. It was also found that PALIANI listed 6303 Champion Road, Chattanooga,

Tennessee, as his home of record beginning January 17th, 2017, on Hamilton County's Sex Offender Registry declaration.

CONCLUSION

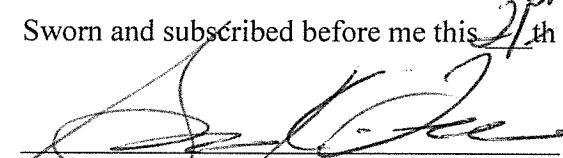
18. Based upon information provided in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and 2252A have been committed and that the items described in Attachment A, attached hereto and incorporated will be found in the subject premises and constitute evidence of violations against the laws of the United States contained within:

6303 Champion Road, Chattanooga, Tennessee 37416.



Samuel K. Moore
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 21st day of Dec, 2018.


SUSAN K. LEE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same including but not limited to:

Any mobile telephonic device, computer, computer system, and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact discs, CD-ROMS, DVD, thumb drives, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, webcams, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
3. Any and all documents, records, e-mails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received.
4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.
5. Documents and records regarding the ownership and/or possession of the searched premises.
6. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

ATTACHMENT B
DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 6303 Champion Road, Chattanooga, Tennessee 37416 is identified as follows:

6303 Champion Road, Chattanooga, Tennessee 37416 is a single family modular residence.

The residence was previously viewed on December 17th, 2018, and photographs were taken of the residence. The residence is a single story modular home on a solid foundation. The home has siding which is tan in color along with a front porch entrance and a side entrance where the driveway terminates that contains stairs and railings. The driveway to the residence is almost directly across from the intersection of Champion Road and Wooten Road.

To reach the residence from Chattanooga, Tennessee, merge onto Riverside Drive and drive approximately 5.8 miles to merge onto TN-17 North. Then drive approximately 2 miles to merge onto TN-58 North staying on TN-58 for approximately 2.4 miles. Upon reaching Champion Road, take a left and continue on Champion for approximately 1.6 miles before reaching the residence which will be on the left.

Attached are photographs of 6303 Champion Road, Chattanooga, Tennessee 37416.

63037



n+Rd,+Chattanooga,+TN+37416/@35.1168345,-85.1635807,3a,75y,347.74h,80t/data=13m611e113m41s71fM3huw8PZiseT3FTT3Ow!2e07i13312!8i6656!4m5!3m4!1s|